

CLAIMS

What is claimed is:

- 1 1. A method comprising:
2 monitoring a state of an image capture system (ICS) while it captures
3 an image of a target;
4 making a digital record of the image;
5 certifying from the record of the image that no unauthorized
6 material alteration of the state occurred during capture of the image.
- 1 2. The method of claim 1 further wherein certifying comprises:
2 encoding the record to allow detection of modification to the capture
3 process and modification of the record itself.
- 1 3. The method of claim 1 wherein certifying comprises:
2 retaining a duplicate of the record of the image; and
3 preventing modification of the duplicate.
- 1 4. The method of claim 1 further comprising:
2 encrypting the record of the image.
- 1 5. The method of claim 1 further comprising:
2 incorporating markers of state in the record of the image.
- 1 6. The method of claim 1 further comprising:
2 preventing subsequent modification of the record of the image.
- 1 7. The method of claim 1 further comprising:
2 maintaining an audit log of access to the record of the image.
- 1 8. The method of claim 7 wherein maintaining the audit log comprises:
2 retaining a log record of at least one of who accessed the record of
3 the image, a location of an accessor, when the record of the image was accessed,
4 and what aspect of the record of the image was accessed.

1 9. The method of claim 7 wherein maintaining the audit log comprises:
2 maintaining a record of parties approving the record of the image.

1 10. The method of claim 1 further comprising:
2 retaining state information corresponding to the capture, wherein
3 the state information includes at least one of: a time of event, an identification of
4 the ICS, a network address of the ICS, a parameter of capture, a local access log
5 and an automatically assigned index.

1 11. A computer readable storage media containing executable computer
2 program instructions which when executed cause a digital processing system to
3 perform a method comprising:
4 monitoring a state of an image capture system (ICS) while it captures
5 an image of a target;
6 making a digital record of the image;
7 certifying from the record of the image that no unauthorized
8 material alteration of the state occurred during capture of the image.

1 12. A method comprising:
2 monitoring a networked image capture system (ICS) while the ICS
3 performs a capture of an image of a target;
4 making a digital record of the image;
5 certifying from the record of the image that no unauthorized
6 material alteration of the state occurred during capture of the image.

1 13. The method of claim 12 further comprising:
2 automatically uploading data captured by the ICS to a remote node.

1 14. The method of claim 12 further comprising:
2 publishing the record of the image to a defined set of networked
3 recipients.

1 15. The method of claim 12 further comprising:

2 maintaining an escrow copy of the data at a remote node secure from
3 modification or destruction to guarantee an authenticity of the data.

1 16. The method of claim 12 further comprising:
2 defining access rights to the digital record of the image.

1 17. The method of claim 16 wherein access rights are automatically
2 defined.

1 18. The method of claim 12 further comprising:
2 enabling the ICS from the remote node.

1 19. The method of claim 12 wherein the monitoring is performed from a
2 remote node.

1 20. A computer readable storage media containing executable computer
2 program instructions which when executed cause a digital processing system to
3 perform a method comprising:

4 monitoring a networked image capture system (ICS) while the ICS
5 performs a capture of an image of a target;

6 making a digital record of the image;

7 certifying from the record of the image that no unauthorized
8 material alteration of the state occurred during capture of the image.

1 21. A method comprising:
2 preventing an unauthorized material alteration of a state of an image
3 capture system (ICS) during a capture of an image of a target;
4 making a digital record of the image; and
5 preventing an unauthorized material alteration of data initially
6 recorded in the record.

1 22. The method of claim 21 further comprising:
2 maintaining an audit log of access to the record of the image.

1 23. The method of claim 22 wherein maintaining the audit log
2 comprises:

3 retaining a log record of at least one of who accesses the record of the
4 image, a location of an accessor, when the record of the image was accessed and
5 what aspect of the image record was accessed.

1 24. A computer readable storage media containing executable computer
2 program instructions which when executed cause a digital processing system to
3 perform a method comprising:

4 preventing an unauthorized material alteration of a state of an image
5 capture system (ICS) during a capture of an image of a target;
6 making a digital record of the image; and
7 preventing an unauthorized material alteration of data initially
8 recorded in the record.

1 25. A method comprising:

2 preventing an unauthorized material alteration of a state of a
3 networked image capture system (ICS) during a capture of an image of a target;
4 making a digital record of the image; and
5 preventing an unauthorized material alteration of data initially
6 recorded in the record of the image.

1 26. The method of claim 25 further comprising:

2 automatically uploading data captured by the ICS to a remote node.

1 27. The method of claim 25 further comprising:

2 maintaining an escrow copy of the data secure from modification or
3 destruction to guarantee an authenticity of the data.

1 28. The computer readable storage media of claim 25 which when
2 executed cause a digital processing system to perform a method further
3 comprising:

4 preventing an unauthorized material alteration of a state of a
5 networked image capture system (ICS) during a capture of an image of a target;
6 making a digital record of the image; and
7 preventing an unauthorized material alteration of data initially
8 recorded in the record.

- 1 29. An apparatus comprising:
2 an image sensing array (ISA) disposed within an assembly; and
3 a data insertion device disposed within the assembly to modify a
4 data stream corresponding to an image capture in a known way.
- 1 30. A method of claim 29 further comprising:
2 an encryption engine disposed within the assembly to encrypt the
3 data stream within the assembly.
- 1 31. A method of claim 29 further comprising:
2 a tamper resistant assembly.
- 1 32. The apparatus of 29 further comprising:
2 a storage unit storing calibration data that defines a signature of
3 inherent characteristics unique to the ISA.
- 1 33. The apparatus of claim 29 wherein the data insertion device
2 comprises:
3 a light source positioned to illuminate a portion of the ISA in a
4 known way during capture.
- 1 34. The apparatus of claim 29 wherein the data insertion device
2 comprises:
3 a optical reference within the apparatus disposed to be imaged by
4 the ISA as a precursor to capture of a target image.
- 1 35. The apparatus of claim 29 wherein the data insertion device
2 comprises:
3 a reader to read pixels of the ISA masked from a field of view of the
4 ISA to generate a pattern substantially unaffected by an image capture.
- 1 36. The apparatus of claim 29 wherein the data insertion device
2 comprises:
3 a plurality of resistors defining a unique electrical signature.

1 37. The apparatus of claim 29 wherein the data insertion device
2 comprises:
3 a memory retaining a marker data set for insertion in the data
4 stream.

T06030" DE 22660